

SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- international: G06F13/00; G06F15/00; H04L9/00; H04L9/00;
H04L9/10; H04L9/12

- european: G06F1/00N7R2; G06F9/445; G06F9/445N;
G06F21/00N7P5M

Application number: JP19910501845T 19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:

WO9209160 (A1)
EP0556305 (A1)
US5222134 (A1)
EP0556305 (A4)
EP0556305 (B1)

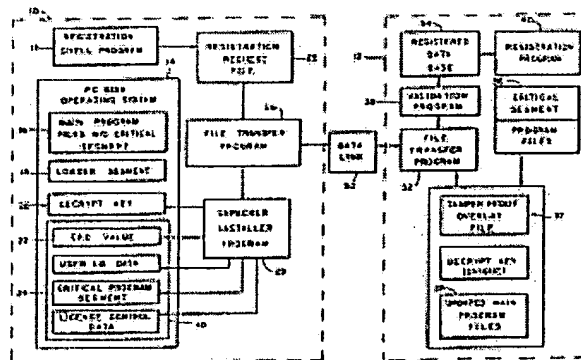
more >>

Report a data error here

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the esp@cenet database - Worldwide

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501120

第6部門第3区分

(43) 公表日 平成6年(1994)2月3日

(51) Int. Cl.

識別記号

片内整理番号

F I

G 0 6 F 13/00

3 5 1 H 7368-5B

15/00

3 3 0 A 7459-5L

H 0 4 L 9/00

9/10

7117-5K

H 0 4 L 9/00

Z

審査請求 有

予備審査請求 有

(全 8 頁) 最終頁に続く

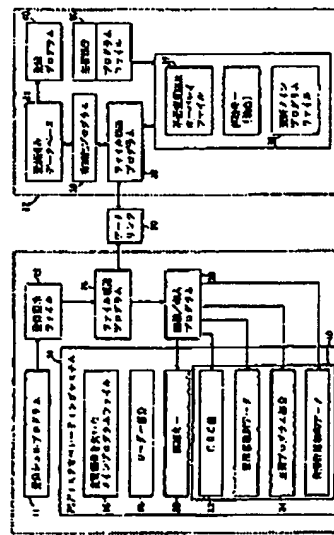
(21) 出願番号 特願平4-501845
 (86) (22) 出願日 平成3年(1991)11月6日
 (85) 翻訳文提出日 平成5年(1993)5月7日
 (86) 国際出願番号 P C T / U S 9 1 / 0 8 0 6 9
 (87) 国際公開番号 W O 9 2 / 0 9 1 6 0
 (87) 国際公開日 平成4年(1992)5月29日
 (31) 優先権主張番号 6 1 0 , 0 3 7
 (32) 優先日 1990年11月7日
 (33) 優先権主張国 米国 (U S)
 (31) 優先権主張番号 6 8 2 , 4 5 6
 (32) 優先日 1991年4月9日
 (33) 優先権主張国 米国 (U S)

(71) 出願人 タウ システム コーポレーション
 アメリカ合衆国 バージニア州 フォルス
 チャーテ, リースバーグ バイク,
 7115, スーツ327
 (72) 発明者 ワイト, デービット, ビー
 アメリカ合衆国 バージニア州 22032,
 フェアファックス ギルバートソン ロー
 ド, 4220
 (72) 発明者 リッデル, ホレイス, ジー
 アメリカ合衆国 バージニア州 22021,
 チャンチリイ, バレイ カウントリ ドラ
 イブ, 13811
 (74) 代理人 弁護士 倉持 裕 (外1名)
 最終頁に続く

(54) 【発明の名称】 パーソナルコンピュータのソフトウェアを適隔位置で起動するための安全システム

(57) 【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルスプログラム(11)が当初備わっている。データリンク(80)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾識別データと使用許諾制御データも含まれている。



第 6 表 平 6-501120 (9)

ファイルは第二レベルの制御機能を有するエグゼクティブ制御プログラムを有しており、

情報を上記登録シミュレーション部分に入力し、

上記使用許諾契約情報と上記登録シミュレーションから独立登録プログラムに送達し、上記登録プログラムは使用許諾契約データを第二レベルの制御機能を有するエグゼクティブ制御プログラムに送達して独自のオーバーレイファイルを作成し、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録シミュレーションに送達し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして

上記独自のオーバーレイファイルを上記登録プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が現在導入されているときだけ可能になることを特徴とする上記のプログラムファイル使用の制御方法。

19. 上記オーバーレイファイルを上記登録用コンピュータから上記登録コンピュータに伝送する以前に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

20. 不正変更防止になっているオーバーレイファイルを伸張する工程を有する請求の範囲第18項に記載の方法。

21. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、送達元検査値を上記暗号化不正変更防止オーバーレイファイル内に提供するとともに解読キーを上記不正変更防止オーバーレイファイルに提供し、上記暗号化および解読キーは上記オーバーレイファイルの独自の内容によって独自に決定されることを特徴とする請求の範囲第20項に記載の方法。

上記登録シミュレーションプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするよう少なくとも一台の登録コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記登録コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記登録コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が現在使われているときだけ、上記プログラムファイルの第二レベルの機能の動作が可能になることを特徴とする上記システム。

22. 上記登録コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル転送過程が上記登録用コンピュータと上記登録コンピュータの両方に図示されていることを特徴とする請求の範囲第21項に記載のシステム。

23. 上記登録用コンピュータが、すべての登録済み使用者が含まれる中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第22項に記載のシステム。

24. オーバーレイファイルを作成するための上記手段が、送達元検査値が記憶されている不正変更防止オーバーレイファイルを作成するための暗号化キーと解読キーとを備えており、上記解読キーは上記オーバーレイファイルと共に上記登録コンピュータに伝送され、上記暗号化および解読キーはファイルの内容によって独自に決定されることを特徴とする請求の範囲第23項に記載のシステム。

22. 新しい送達元検査値が、上記オーバーレイが実行のためにロードされるたびに新装されて、上記オーバーレイファイルと共に送達された送達元検査値と比較され、上記オーバーレイファイルが作成以降変更されているかどうかを判断することを特徴とする請求の範囲第21項に記載の方法。

23. 上記使用許諾契約情報と上記オーバーレイファイルが、上記登録シミュレーションと上記登録プログラムとの間に電子データリンクを介して伝送されることを特徴とする請求の範囲第22項に記載の方法。

24. 上記登録シミュレーションプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに図示されていることを特徴とする請求の範囲第23項に記載の方法。

25. 上記有効化により上記使用許諾契約情報が正式に登録シミュレーションに有効であることを特徴とする請求の範囲第24項に記載の方法。

26. 上記使用許諾契約情報と上記オーバーレイファイルが一台のコンピュータに導入され、備えもれることを特徴とする請求の範囲第25項に記載の方法。

27. 制限されたあるいは制限されない期間、プログラムファイルとアップグレードするシステムにおいて、

第一レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが送達されて、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記送達コンピュータは登録シミュレーションプログラムが図示され、

システム。

21. 上記登録コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためのロードされるたびに新しい送達元検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に送達された送達元検査値と比較するための手段を備えていることを特徴とする請求の範囲第20項に記載のシステム。

【 明 細 書 】

パーソナルコンピュータのソフトウェアを遠隔位置で起動する
ための資金システム

発明の背景

一般的に、パーソナルコンピュータあるいはそれに類似した装置の使用者の大部分は、それら装置で実行するソフトウェアを様々な小売店からあるいは通信販売を通じて入手する。いずれの場合も、ソフトウェア製品はいわゆる「紙箱包装」材で包装されており、その紙箱包装材を開いた時点でそのソフトウェア製品に対する使用許可契約が成立して、その製品の使用許諾者も使用許諾者／購入者による使用許可契約あるいは使用から保護するようになっている。この方法による商行為は、許諾者と使用許諾者の双方にとって満足すべきものではないことが分かっている。たとえば、使用許諾者にとっては、ソフトウェアプログラムを動作させてみてからそれが使用許諾者が必要としているものかどうかを判断する機会が与えられない。さらに、許諾者の側からみると、この方法では使用許諾者の識別が難しく、許諾者によるプログラム使用の制御あるいは監視を行なうことができない。

ソフトウェアプログラム保護方法は、Thomasの米国特許第4,446,519号に図示されており、プログラムと記された「はい／いいえ」で書える質問がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに設置されているハードウェアあるいはファームウェア保護装置の存在を判断するようになっている。この装置の意図は、プログラムが物理的な複製をなしでは使用できないようにすることであり、これはソフトウェアよりも複製することがはるかに困難である。しかし、このような方法は、正しい符号化形式が見破られ、そしてそれをかすかに変更してプログラムに書き込まれてしまえば、簡単に打ち破られてしまう。ひとたび打ち破られると、無制限の違法コピーが作成され配布される可能性がある。

特許平6-501120 (4)

Williamの米国特許第4,740,830号は、中央（遠隔）コンピュータを記憶して、正しい符号の入手を試みる意図のプログラムがアクセスできないマスターリストあるいはアルゴリズムから得られたコード解除コードあるいは有価化コードを生成することを開示している。しかし、この方法は、任意のコードを受容することにより、あるいは保護の周囲をプログラミングすることにより、もしくはデバッガープログラムによりプログラムを分析してプログラムの実行を可能にするコードの存在を見つ出すことにより、簡単に見破られてしまう。ひとたびこの保護が打ち破られると、動作可能なプログラムの無制限のコピーが作成され配布される可能性がある。

さらに、Schoidの米国特許第4,649,510号に開示されている方法では、最も価値のあるアルゴリズムを無効化し、無効化されたプログラムを地帯装置内で実行すると同時に、回復アルゴリズムを別の物理的に分離し保護された処理装置で実行することにより回復し、有効装置をよつて処理部の相互関係によって獲得するようになっている。このような方法は、回復アルゴリズムの物理的保護に依存しており、この物理的保護が侵害された場合、意図のプログラムによって簡単に打ち破られる可能性がある。したがって、そのような方法は、回復記憶媒体の物理的保護が維持できない大量市場においては、実用的ではない。

そのため、ソフトウェアを容易に使用から保護しつつソフトウェアを大量市場に配布するための経済的な方法が求められる。さらに、見込み購入者／使用許諾者がソフトウェア製品を購入前に試してみることができよう方法とシステムも必要である。また、ソフトウェア製品の改良および更新部分と登録使用許に配布するための方法も必要である。

発明の要旨

本発明は、パーソナルコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理する方法で配

布する方法とシステムに関する。動作可能なプログラムは、購入者／使用許諾者と販売者／許諾者との間の特定の契約において入手可能になる。販売者と購入者との関係は、本発明の目的に照しては、許諾者／使用許諾者の関係である必要はないが、以下では販売者を許諾者、購入者を使用許諾者もしくは使用者と呼ぶ。ひとたび使用許諾者が特定の契約条件に同意すると、使用許諾者識別データが登録用コンピュータに与えられる。登録用コンピュータはその契約を記憶し、使用許可されたプログラムの可動部分を生成する。これらの部分は不正変更防止が施されていると同時に、識別された使用許諾者にとって独自のものとなっている。この情報の交換に基づき、可動コンピュータプログラムが登録済み使用許諾者のコンピュータに不正変更防止ファイルに格納されて戻される。同時に、このファイルには使用許諾者独自の情報が含まれている。本発明の実施例としては様々なものが考えられるが、いずれの実施例も使用許諾者を識別する独自のデータと格納されているソフトウェアプログラムに関する情報とが含まれている暗号化パッケージの形態を伴っている。したがって、使用許諾者は署名ではなく、そして格納されたソフトウェアは使用許諾者によって署名された暗号化パッケージに含めることにより、様々な制度を設けて使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能のあるマーケティングシミュレーションプログラムの最初の配布が伴う。このシミュレーションプログラムは、見本版と直接記述だけを有しているか、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローダーセグメントと呼ばれる特定のプログラムモジュールを含むような構成になっている。

マーケティングシミュレーションは適切な方法で自由に配布されるであろう。マーケティングシミュレーションがプログラムのデモンストレーション

版を有している場合、ニグゼクティブ知識グループが保護されたプログラムの固定版になる。マーケティングシミュレーションは見込み使用者に登録を促す。マーケティングシミュレーション内の登録プログラムは、登録データと登録データベースコンピュータに中継する。暗号化ファイル内で格納された使用許諾者独自のデータと動作可能版のプログラムとを有する独自の暗号化パッケージが組み立てられる。独自の暗号化暗号キーが、暗号化ファイルおよび格納されていないプログラムファイルと共に使用者のコンピュータに伝送される。これらのマーケティングシミュレーションを最大化させる。暗号キー、暗号化ファイル、そして格納されていないファイルの形態と同時に、マーケティングシミュレーションはこれらの各々を使用者のコンピュータに導入する。

したがって、使用者がプログラムを実行する毎に、ローダーセグメントが提供された暗号キーを使用して、暗号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解放する。このプログラムは保護されていないソフトウェアプログラムの設計にしたがって実行され、独自の使用許諾データもプログラム実行中にロードされる。プログラムが実行されていないときは、保護されているプログラムはその暗号化形態に留まって、格納されていないプログラムファイルと共にコンピュータの大量記憶装置に格納されている。保護されているプログラムは実行のためにロードされたときだけ解放され、正しい暗号化キーにアクセスしなければ実行され得ない。

図面の簡単な説明

- 図1は本発明による従来の構成を示す流れ図である。
図2は本発明によるプログラム実行過程を示す流れ図である。
図3は、本発明の図1による代表的なパーソナルコンピュータと登録用コンピュータの関係図である。
図4は、本発明の図1による代表的なパーソナルコンピュータと登録用コンピュータに代る実施例を示す関係図である。

利用の目的と範囲

本利用の目的は、許諾者がそのプログラムの費用対効果に関する費用を従事使用されている方法よりはるかに効率的な方法で維持することを可能にすることである。さらに、本利用の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る前に試用することも可能にすることである。さらに、本利用の更なる目的は、特定のプログラムの使用許諾保護されたソフトウェアと並んで製品被許諾者に配布する手段を提供することである。したがって、本利用の知見は包括的なものと考えられ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと仮定されている。

一実施例において、動作可能なエグゼクティブ制御ループを除いて完全な製品プログラムが、パーソナルコンピュータあるいは他の装置において、磁気ディスク、フロッピーディスク、ハードウェアあるいは他の不揮発性記憶装置に提供される。さらに、この特定のプログラムには登録シリアルプログラムが含まれる。ただし、小さいプログラムもしくは単に低性能のあるプログラムの場合、プログラム自体は保存せず、シリアルだけが提供される。エグゼクティブ制御ループが除外されているため、このプログラムは正しい登録過程を実現しなければ動作しない。図1および図2に示されているように、この登録過程は、パーソナルコンピュータ(PC) 10内部の登録シリアルプログラム11と登録用コンピュータ12内部に提供されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピュータ12内に提供され、電子データリンク30を介して登録シリアルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話モデムリンクでもよく、あるいはその他のいかなる媒体であってもよい。ただし、第二の実施例においては、登録シリアルおよび登録システムプログラムは同一の媒体上に格納されてもよいが、その媒体は製品応用プログラムとは別でなければならぬ。この場

特表平6-501120(5)

合、登録シリアルおよび登録システムプログラムが入っている非揮発性媒体は、許諾された購入プログラムによって使用者パーソナルコンピュータ10へ個人的に移植され、電子データリンクは必要ではない。

登録シリアルプログラムは、使用者がPCオペレーティングシステム14のメインプログラムファイル内に提供されている製品応用プログラムの実行を最初に実行すると実行される。登録シリアルは、製品応用プログラムに関する追加情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を促して候補者として登録する。使用許諾は、特定の追加情報における特定の被許諾者に対して提供され、その期間は無条件または一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シリアルは、不正変更防止スーパーレイファイルが存在しないかぎり、メインプログラムを実行しない。登録シリアルプログラム11は、被許諾者のPCに表示されるデータ入力形式を提示し、被許諾者に対して、請求書送付先、口座番号、使用許諾条件などの個別情報の提供を要求する。この情報は、被許諾者が再帰する登録要求ファイル25に入力される。そして、登録シリアルプログラムは、被許諾者が特定のキーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが開き、そして登録シリアルファイル転送プログラム26が登録システムファイル転送プログラムとのデータリンクを確立する。登録用コンピュータ内の登録プログラム40は、データリンクが正当な登録シリアルで確立されていることを確認する検密保護チェックを実行する有効化手段41によって保護される。つぎに、登録シリアルは登録要求ファイル25を、そのファイルを受信する登録システムに転送し、必要なローテーションと、結合されたファイル転送プログラム28および32間のハンドシェイク動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受信されると、登録要求が登録済み利用者34のデータベースに対して格納される。確認には、その要求に答えるべきかど

うかを判断する様々なチェックが含まれる。たとえば、一時的使用許諾に対する要求が特定の被許諾者から再度送られてきた場合、その被許諾者には使用許可が与えられず、そしてそのプログラムのエグゼクティブ制御ループは過剰されない。そのような状態が完了した場合、通知メッセージが登録シリアルに転送され、見込み被許諾者に対して表示される。しかし、要求が確認されると、登録済み利用者データベースへの登録が決定されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ12の内部では、つぎに使用許諾データが使用されて、使用許諾データとエグゼクティブ制御ループプログラム命令35とを結合することにより作成された独自の不正変更防止スーパーレイファイルが生成される。結合されたデータとプログラムファイルに各自で、不正変更防止スーパーレイファイル37内に含まれる巡回冗長検査(CRC)値が計算される。一組の独自の暗号化キーと解読キーが作成され、不正変更防止スーパーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正変更防止スーパーレイファイルと共に提供される解読キーが提供される。暗号化アルゴリズムは、同期暗号化システムのように、暗号化と解読にそれぞれ異なるキーを使用する状態であればなんでもよい。登録システムが、不正変更防止スーパーレイファイルと解読キーを、パーソナルコンピュータ登録シリアルに転送される1個のデータファイル38に格納込む。また、更新されたメインプログラムファイルもこのデータファイルに格納込まれ、ファイル転送プログラムとすでに確立されているデータリンクとを介してPCの登録システムに転送される。

出荷ファイル一式の受取と同時に、登録シリアルプログラム内の開梱-導入プログラム39が他面ファイルを開き、エグゼクティブ制御ループセグメント36、CRC値32ならびに解読キー30および、含まれている場合は、更新されたメインプログラムファイルを含む不正変更防止スーパーレイファイル40を導入する。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する請求が、中央登録用コンピュータ12にかける別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された配布済み製品応用プログラムを起動して、不正変更防止スーパーレイファイルと解読キーを使用して製品応用プログラムを実行するたびに実行する製品応用プログラム一式をロードするためのプロセスが開始される。

このプログラム実行過程を図3に示す。図示されているように、パーソナルコンピュータの使用者が製品応用プログラムの実行でオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラム命令に先立って実行される。つぎに、ローダーセグメントは製品応用プログラムの起動を実行し、不正変更防止スーパーレイの存在をチェックする。不正変更防止スーパーレイが導入されていないければ、ローダーセグメントは終了してオペレーティングシステムに戻る。メインプログラムファイルの実行が事前に禁止される。不正変更防止スーパーレイが導入されていれば、ローダーセグメントは解読キーを見つけて不正変更防止スーパーレイの解読とロードを行ない、メインプログラムファイルに対して存在しないエグゼクティブ制御ループプログラム命令ならびに独自の解読および使用許諾制御データを合わせる。解読が完了すると、巡回冗長検査とCRC値が実行され、それが完了すると、不正変更防止スーパーレイが登録済みコンピュータからパーソナルコンピュータに格納されたときに作成された不正変更防止スーパーレイに記憶された巡回冗長検査値と比較される。巡回冗長検査値が失敗に終わると、そのスーパーレイは知らぬ方法によって変更が加えられたものとみなされ、したがって無効とされる。この時点で、ローダーセグメ

特表平6-501120 (B)

ントはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイのどの部分も変更されていても、事前に防止される。返戻冗長検査の意思、オーバーレイが変更されていないことが確認されると、ローダーセグメントはオーバーレイを含むメインプログラムファイルの実行を開始し、そして製品応用プログラムが最後まで実行される。

不正変更防止オーバーレイは動作可能状態の製品応用プログラムに含めることを要することにより、被読者範囲と使用許諾制御データがそれ以降動作可能プログラムに共に含まれることになる。このようにして、読者は不正使用を防止するとともに監視することが出来る。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのエグゼクティブ制御ルーブセグメントと使用許諾制御データを含む不正変更防止オーバーレイファイルが生成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動時に不正使用を防止するキー記憶である。なぜなら、エグゼクティブ制御ルーブプログラム命令は、完全なには独自の使用許諾制御データと使用許諾制御データから分離することのできなければ、被読者範囲と使用許諾制御データも完全なには複製できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが生成される時に最初に返戻冗長検査値をオーバーレイファイルに記憶させると不正変更防止になるとみなされる。返戻冗長検査値は、プログラム命令と使用許諾データを組み合わせたオーバーレイファイルの内容全体に対して計算される。被読者範囲データは製品であるので、各々のCRCは製品自体のうちに、記憶されている。

もCRC値が、オーバーレイがロードされるたびにローダーセグメントによって計算された返戻冗長検査値と比較される。これらの返戻冗長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容になんらかの変更が加えられていれば、記憶されている返戻冗長検査値に一致する変更が行われなければ、そのオーバーレイファイルは無効になる。つぎに、不正変更防止オーバーレイの内容全体が、返戻冗長検査値の位置が不明になるような方法で暗号化されるので、この値の所在を突きとめてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令ならびに独自の被読者範囲および使用許諾制御データがはっきりしなくなる。暗号化は、公開暗号化システムのように暗号化と復号化に別々のキーを使用する技法によって達成される。暗号化ならびに独自の暗号化キーおよび解読キー発出のためのアルゴリズムは登録システム内に基礎し、したがって被読者にはアクセスが不可能である。解読キーは、登録システムと登録プログラムシェルの通じて被読者のコンピュータに提供される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することは、困難ではあるが可能である。しかし、内容を複製して、新しい複製されたオーバーレイファイルを暗号化する試みは、暗号化キーに属するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけでは公開暗号化キーで解読できず、私的キーは公開キーから容易には導出されないというのが、公開暗号化システムの特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ルーブセグメントと、使用許諾の方法と制御に適切な独自の使用許諾制御データを有している。このデータには、

演習期間の期間、コンピュータの製造番号、コンピュータのモデルの電話番号、そしてその他の情報が含まれる。

ローダーセグメント18は登録目的のサブプログラムであり、これは、ローダープログラムが取り除かれたり返戻された場合、メインプログラムファイルを動作不能にする技法によって製品応用プログラムのメインプログラムファイルに結合される。この結合技法は、特定のプログラム命令と製品応用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内蔵された命令は、使用者にとっては未知の記憶位置にある特定の値を検査する。ローダープログラムセグメントを実行すると、特定の値がメインプログラムファイルの動作を可能にするのに必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の適性の知にこの動作を支持する。したがって、ローダーセグメントを取り外したり返戻したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

図3の実施例において、登録シェルは、製品応用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一部として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解読キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の使用許諾データは含まれないが、登録版の製品の複製と表示のデモンストレーションだけを行なうメインプログラムエグゼクティブ制御ルーブが含まれるであろう。デモンストレーション版のエグゼクティブ制御ルーブは、エグゼクティブ制御ルーブの複製設計によって得られたプログラムの様々な特性を有している。たとえば、複製版を提供するデモンストレーションコンピュータをプログラムングして演習版を表示することが出来るが、デモンストレーション版のエグゼクティブ

制御ルーブをプログラミングして演習版を製品登録依頼として解釈して、製品を動作させる前に登録することを要求できる。

登録を開始する前に、見込み被読者はプログラムを実行し、デモンストレーション版が実行されよう。固定して図4に示したように、デモンストレーション版の解読キーが使用され、デモンストレーション版のエグゼクティブ制御ルーブがロード、解読、そして実行される。デモンストレーションが終了すると、見込み被読者は、使用版として登録し登録版のプログラムを支持するための一時的な使用許諾を得るようになる。そして、使用者は前述のようにして登録を行い、図4に示されているプロセスを開始することができる。登録要求に応答して、新しいオーバーレイファイル40'と独自の解読キー20'が含まれている公開ファイルが登録用コンピュータから送られる。このプログラムファイルと更新版のプログラムファイルも、出荷ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解読キー20をそれぞれの登録版40'と20'で置き換える。

登録に続き、使用者がプログラムを実行すると、プログラム実行過程で登録版の不正変更防止オーバーレイ40'が検出されてロードされ、独自の解読キー20'を使用することにより、登録版のエグゼクティブ制御ルーブが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に交換される。

プログラムの複製向上版が利用される場合、使用者は同一のプロセスを移動してさらに別の解読キーと、より強化されたエグゼクティブ制御ルーブと追加プログラムファイルを含む不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することができる。

様々な実施例が、小さな不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための適当な複製技法を提

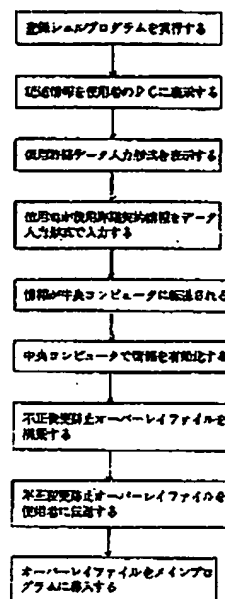
拍表平6-501120 (7)

用することが出来る。このような技術は、ここにも含まれているように、プログラムの部分あるいはプログラム全体を使用所実装と結合する形式で配布するための、ここに開示されている方法がもたらす高度所利益の可能性の單なる例である。

上記の知見に照らし合わせ、本発明に最も適する例が可成り分
ことは明らかである。たとえば、本発明は、使用者のコンピュータ
がその地域の登録用コンピュータに接続され、さらにその登録用
コンピュータがそれより広い地域の登録用コンピュータに接続さ
れ、というように階層構造内に実装することも可能である。その
地域の登録用コンピュータの登録範囲は、その地域の登録用コン
ピュータとそれより広い地域の登録用コンピュータとの範囲に含
まれる登録非制限ゾーンによって制限できるであろう。したが
って、下記の発明の態様に於ておれば、本発明と上記記載書に
記載されている以外の方で実施することができらる。

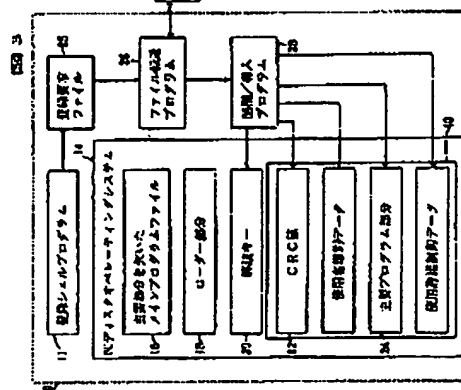
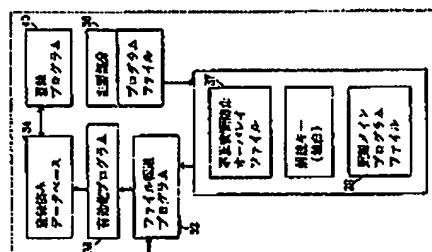
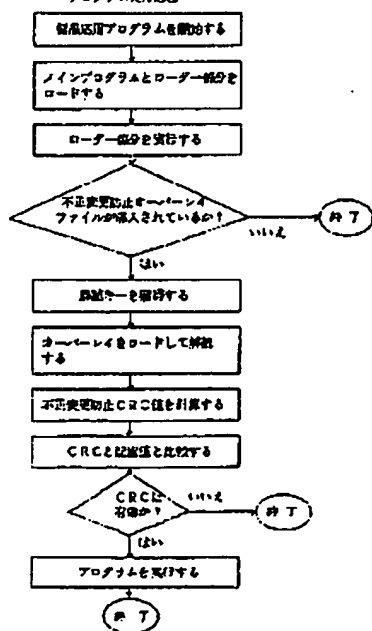
50 3

● ● ● ●

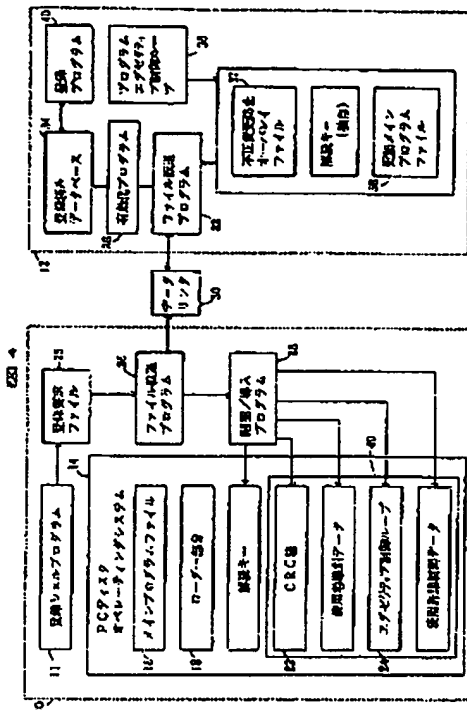


23 2

アセトナール



特賣平6-501120 (8)

[illegible]

フロントページの読み

(SI) Int. Cl. ⁸
H04L

識別記号 庁内整理番号

F 1

(61)指定国 BP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, S E), CA, JP